eHealthcare
STRATEGY & TRENDS

Internet Management, Marketing, Analysis, and Intelligence

Focus on Privacy/Tracking

Strategies to Navigate the Risks and Maintain Compliance

An Exclusive Special Report from
eHealthcare Strategy & Trends

plain english HEALTH CARE

eHealthcareStrategy.com

Sponsored by
Freshpaint

Additional copies can be purchased at:
https://ehealthcarestrategy.com

Plain-English Media, LLC
custserv@plainenglishmedia.com

(866) 641-4548
909 Marina Village Parkway #183
Alameda, CA 94501

A Message from the President

Dear Healthcare Marketing Leader,

In an era dominated by digital advancements and data-driven strategies, privacy and tracking have become significant areas of concern for healthcare marketers and communicators. As hospitals and health systems increasingly embrace digital platforms for marketing and communication, healthcare marketers and strategists must navigate a delicate balance—leveraging the power of targeted marketing and personalization to engage audiences while safeguarding the sensitive nature of health information.

The challenges lie not only in complying with recent online tracking regulations, but also in building and maintaining trust with consumers who are becoming more concerned about data security and how their personal information is used.

In this new report from *eHealthcare Strategy and Trends*, you'll get a comprehensive look at the current privacy/tracking landscape in healthcare marketing. Through expert insights and in-depth interviews, we'll provide you with practical tips and strategies to help you navigate the complexities of privacy and tracking in your healthcare marketing efforts.

Specifically, you'll learn:

- Guidance from Atrium Health on how to balance privacy, security, and usability in your marketing strategy.
- Six immediate actions you should take to respond to the 2022 HIPAA guidance on online tracking technologies, plus advice from a legal expert.
- Insights from WebMD Ignite on how to manage online tracking technologies and safeguard sensitive healthcare data.
- Five ways to measure ROI and growth beyond tracking pixels.
- A comprehensive look at possible workarounds from Ben Dillon that can help marketers achieve measurable, trackable, and effective marketing, in compliance with HIPAA.
- Advice from Freshpaint on how to assess your current situation regarding tracking technologies, protect your patients' privacy, and help your organization steer clear of HIPAA violations — plus four tips for compliance.
- Why Anthony Katsur, CEO of IAB Tech Lab, believes privacy enhancing technologies can be a potential solution to privacy in AdTech.

Our goal for this report and all eHealthcarestrategy.com content is to give you tools and tips, information and inspiration to develop your skills as a leader. We are confident that you will find high value, actionable ideas you can put to work for the benefit of your organization.

For more expert guidance that will help you stay current with emerging trends, visit ehealthcarestrategy.com today.

Best regards,

Matt Humphrey
President
Plain-English Media
Publisher of eHealthcarestrategy.com

Table of Contents

Freshpaint

Embrace Privacy, Elevate Performance: The Freshpaint Path to HIPAA-Compliant Healthcare Marketing

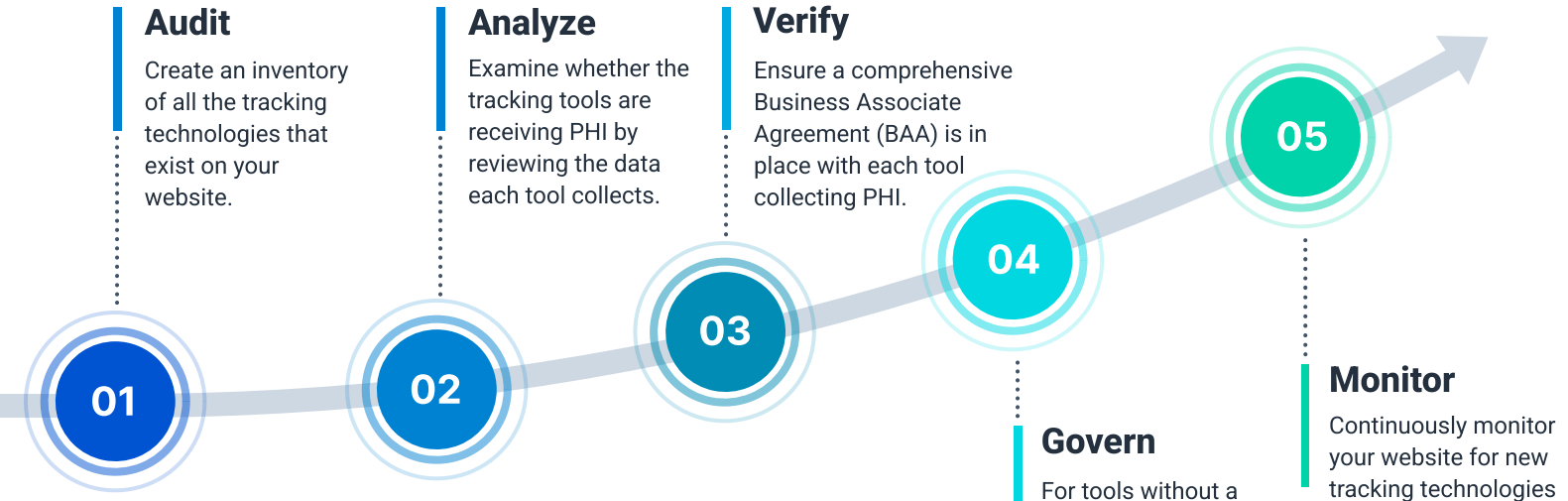
“It felt like a death in the family for us.”

That was Columbus Regional Health’s reaction to the HHS guidance about the use of online tracking technologies. Their dramatic reaction wasn't unique, as healthcare organizations nationwide faced similar panic, with fears of potentially needing to lay off advertising and analytics teams as a result of the guidance.

However, a deeper analysis revealed that the guidance actually offered an opportunity. Healthcare organizations embracing this new directive gained a competitive edge. All they had to do was make a strategic shift in marketing from an "outcome-first" to a "privacy-first" approach.

A Privacy First Framework

Lock down the tracking tech on your website



Audit

Create an inventory of all the tracking technologies that exist on your website.

Analyze

Examine whether the tracking tools are receiving PHI by reviewing the data each tool collects.

Verify

Ensure a comprehensive Business Associate Agreement (BAA) is in place with each tool collecting PHI.

Govern

For tools without a BAA, use a Healthcare Privacy Platform to govern the flow of PHI to those tools.

Monitor

Continuously monitor your website for new tracking technologies that might be added and ensure they comply with the privacy-first approach.

Freshpaint

Embrace Privacy, Elevate Performance: The Freshpaint Path to HIPAA-Compliant Healthcare Marketing

Freshpaint enables this privacy-first approach through our industry-first Healthcare Privacy Platform.

The platform is designed to:

- Find and flag all web tracking technologies that exist on your website.
- Help you understand the data that is being passed to marketing tools.
- Be safe-by-default by not sharing any PHI with non-compliant tools.
- Preserve the visitor journey without violating privacy rules.
- Allow healthcare marketers to use analytics tools like Google Analytics in compliance with HIPAA.
- Unlock the power of ad platforms, like Meta ads, while maintaining HIPAA compliance.

More than 100 healthcare organizations, like Columbus Regional Health, have started using Freshpaint's Healthcare Privacy Platform to take a privacy-first approach to their marketing.

With the help of our platform, healthcare systems are able to:

- **Find and remove non-compliant web trackers:** The Healthcare Privacy Platform identifies all non-compliant web trackers so healthcare organizations can remove the trackers from their websites.
- **Get back online:** For organizations like Columbus Regional, it takes only 20 days to go from non-compliance to full compliance for Google Analytics and other well-established marketing tools.
- **Improve performance:** Healthcare organizations using the Privacy Platform are seeing an improvement in ad performance because of additional HIPAA-compliant use cases that can be unlocked.

Freshpaint helps healthcare organizations unlock HIPAA-compliant, high-performance marketing.

Learn how at freshpaint.io

Learn More

TRUSTED BY HEALTHCARE

Modern Health · New York Proton Center · vybe urgent care · Columbus Regional Health · Baptist Health

The Impact of Online Privacy and Security on Health System Brands — and How You Can Lead

By Jane Weber Brubaker

Which would you prefer to be known as — a health system that makes things easy for consumers and can be trusted to safeguard their data? Or one that adds friction in the name of security, and puts personally identifiable information at risk?

There are so many ways data, or lack of data, can get you in trouble these days.

If you're the CIO, you're constantly guarding against potential data breaches and ransomware attacks. If you're the CMO, you're worried about how you're going to deal with a cookie-free world. And if you're a patient or consumer, you want great online experiences that make every task easier, but you don't want companies playing fast and loose with your personally identifiable information (PII).

There is no shortage of internal and external threats, challenges, and changes — an employee who opens an attachment in a phishing email, bad actors looking for vulnerabilities to exploit, new privacy legislation, and Big Tech companies trying to outdo each other in defining the new rules of consumer privacy. There are more devices than ever, and since the pandemic, virtual care is commonplace, adding to potential vulnerabilities and disconnected experiences.

How your health system navigates these choppy waters — and they're only becoming more treacherous by the day — will determine how consumers view your brand.

Great online experiences are important to consumers, but so is privacy. Does it have to be either/or?

One category of privacy and security solutions, CIAM, or customer identity and access management, claims to support friction-free experiences without compromising consumer privacy or the security of digital properties they engage with.

Pablo Suarez, field CTO (Healthcare) at WSO2

In a Reuters Events webinar in early August, "Elevate Your Health Data Stewardship and Enhance Patient

Experiences with Secure Digital Interactions," Pablo Suarez, field CTO (Healthcare) for identity resolution provider WSO2, said, "To deliver the digital experiences that we call digital transformation … we need more secure digital data sharing to occur. The adoption of a CIAM platform to secure the digital front door, and at the same time, enable a frictionless user experience, I think that's how we're going to reach digital transformation in healthcare."

Suarez was joined by senior technology leaders from Atrium Health, Permanente Federation, and AdvantageCare Physicians, who weighed in on the current threat-filled environment. To sum it up, the bad guys are getting smarter. The stakes are high when it comes to online privacy. Once the trust is broken, it's almost impossible to regain.

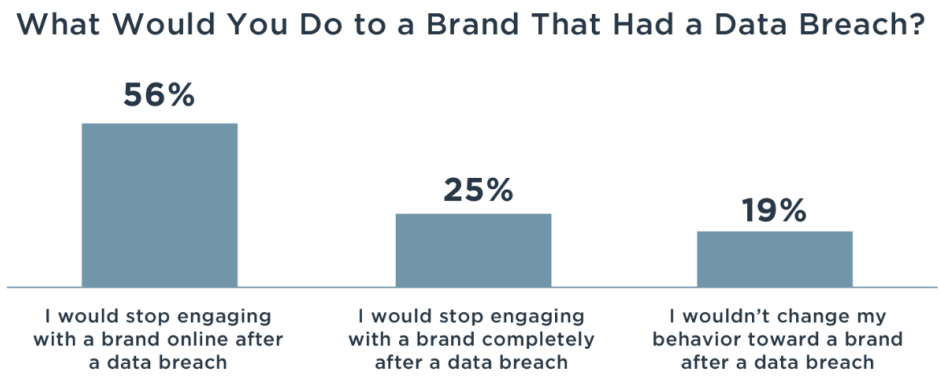
Andy Crowder is SVP and chief information and analytics officer at Atrium Health. "We've got a sacred relationship with patients and customers. They trust us," he says. "It's about being able to care for people in their greatest time of need. And when that's compromised, it is a significant impact to our brand and the loss of trust that those customers and patients give us, and so it's not just about the financial implication, and hit to revenue, it's about our ability to care," he says.

Andy Crowder, SVP and chief information and analytics officer at Atrium Health

Crowder was specifically referring to disruptions affecting clinical care, but any poor experience can frustrate consumers and drive them away, whether it happens while paying a bill or checking in for an appointment. A 2018 report from PwC found that "32 percent of customers say they will walk away from a brand they love after just one bad experience." And a data breach would drive most consumers away for good.

Privacy as Part of the Marketing Strategy

Marketers are deeply concerned about creating experiences that delight consumers, but they don't typically think of privacy as part of the mix. What if they stopped seeing privacy as an obstacle to overcome and instead saw effective privacy management — and leadership — as a strategic opportunity that would raise an organization's profile and stature.



A 2019 report from Ping Identity found that 81 percent of consumers would drop a brand after a data breach.

Consider the example of Apple staking out a leadership position on privacy. Apple shook up Big Tech when it preemptively gave consumers using its Safari browser control over how their information is shared. The company became the white knight of consumer privacy, leaving its competitors to play catchup.

A 2021 Forrester report commissioned by Neustar, "Transforming Customer Data Management: Bridging the Gap Between Consumer Privacy and People-Based Marketing," makes the point that "[w]hile brands are keenly aware of the shifts happening in customer data, they struggle to meet the moment with comprehensive, identity-based strategies that would let them simultaneously tackle issues of privacy management, data governance, and marketing management."

Balancing Privacy, Security, and Usability

As third-party cookies become a thing of the past, can customer identity and access management solutions help brands, including health system brands, build trusted relationships with consumers and pave the way for seamless, frictionless, personalized journeys based on one centralized profile? Even the best of these solutions is still evolving, but typically would include these features:Customer registration

- Self-service account management
- SSO (single sign-on)
- MFA (multi-factor authentication)
- Preference and consent management
- Access management
- Directory services
- Governance of data access

Source: CIAM: What is customer identity and access management?

Going back to the Reuters Events webinar, it is an ongoing challenge to find a balance between protecting privacy and security and raising the bar so high that patients and consumers throw up their hands in exasperation. Atrium Health's Crowder says, "We don't want to make that barrier so high to prevent the threat actors but also alienate a particular customer base we've got that we still have an obligation to take care of."

Jane Weber Brubaker is executive editor of Plain-English Health Care, a division of Plain-English Media. She directs editorial content for eHealthcare Strategy & Trends *and* Strategic Health Care Marketing*. Email her at jane@plainenglishmedia.com.*

Back to Table of Contents ▲

HIPAA Compliance 2023: A Guide to Google, Meta, and Other Online Tracking Tools

By James A. Gardner

In December 2022, the Office of Civil Rights put the hammer down, shoring up HIPAA regulations to cover online tracking technologies that could compromise consumer privacy. Healthcare marketers must take a proactive role in responding.

Healthcare marketing is full of important acronyms, but HIPAA — the federal Health Insurance Portability and Accountability Act of 1996 — truly stands alone. Confusingly vague, often misunderstood, and yet backed by stiff penalties, overlooking the HIPAA rules for protecting personal health information is done at your peril.

Like me, you were probably surprised early last summer when The Markup and STAT+ assessed the websites of 100 prominent hospitals. On a third of them, they found user tracking technology from Meta — the parent company of Facebook — that was apparently capturing data about pages visited, searches conducted, appointment scheduling, and so forth. Seven of the health systems had installed Meta Pixel code in their patient portals, exposing Protected Health Information (PHI).

The combination of health information being shared non-consensually with a third party alongside uniquely identifiable information like an IP address alarmed many. It raised the possibility of, say, a sensitive search for a mental health condition or emerging cancer becoming known to Meta and its advertising algorithms.

"It is quite likely a HIPAA violation," noted David Holtzman, a health privacy consultant who previously served as a senior adviser in the U.S. Department of Health and Human Services' Office for Civil Rights (OCR), which enforces HIPAA.

OCR then further upped the ante for healthcare marketers in December when it released important new guidance on all online tracking technologies.

Some form of tracking is essential for marketers. What is a reasonable response to the risks? Concern, not alarm, should be your tone when engaging your organization's leadership. Read on to learn the six immediate actions you should take to get in front of this, and some possible alternatives to Google and Meta tracking tools.

OCR's bulletin, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, emphasizes, "*While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for*

regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule."

The bulletin continues, "*All such information collected on a healthcare provider's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the data collected, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of healthcare services.*"

The message is clear: All our old compliance assumptions about online tracking tools — everything from Google and Meta to HotJar and Microsoft — need to be revisited. Ignore the new guidance and risk an enforcement action or civil lawsuit. Many of us began to worry.

For a not-eager-to-get-into-trouble healthcare marketer — that's everyone, I hope! — what's a reasonable approach to all this?

First and most important, **engage your marketing, legal, privacy, and/or compliance leadership** if you haven't already. They may choose to consult a trained HIPAA attorney. Don't know the right resource? Contact me for a trusted recommendation.

In tandem, here are six immediate actions you can take:

1. **Get smart on tracking tools and OCR's thinking.** You'll be expected to understand them and help lead your team's thinking. What exactly are tracking tools? Why do we use them? What's OCR's concern here?
2. **Remove unused and forgotten tools.** Audit your websites and apps regularly to understand the tracking technologies you currently use. Document them and remove any you don't recognize or no longer use.
3. **Understand what your tools share.** Ignorance is not an excuse; you are responsible for knowing where your tools are deployed, what data is collected, where the data is being transmitted, and limits on use of that data. You may need to consider filing a breach notification if you've inadvertently been noncompliant.
4. **Make a case for your essential tools.** Ensure trade-offs are understood as tools are eliminated from your toolkit. Some tools are critical for successful online marketing, and this needs to be made clear. Expect to be asked what other organizations do.
5. **Pursue HIPAA compliance where possible.** Some partners — not Meta or Google, unfortunately — will help your efforts to become HIPAA compliant by signing a Business Associate Agreement (BAA).
6. **Scrutinize all future tracking technologies**. Going forward, review all technologies from third parties with your privacy and compliance teams. No tools should be deployed without an assessment of their value and risk.

Where might this all shake out in 2023 and beyond?

There are many types of tracking tools, but those from Google Analytics and Meta are causing the most angst among healthcare marketers. They're ubiquitously deployed and are close to essential to many marketing teams.

I believe we'll see a range of decisions.

Many organizations have already pulled back on Google Analytics, Meta, and all but the most benign technologies while the dust settles. More than a few already operate their websites and apps with no analytics or measurement tools at all.

Other organizations may have found a different balance.

Some have configured Google Analytics to anonymize IP addresses before they're stored, an approach OCR discourages in its guidance. A breach can occur based only on the fact that data is transmitted to a third party, even if not viewed or used.

Others are exploring the next-gen Google Analytics 4 (GA4) platform, which claims to not log or store IP addresses at all. But there are concerns here, too. Other identifiable information is being collected and even the transmission of data can be problematic, skeptics point out. Google (and Meta, for that matter) make no claims of being HIPAA compliant and are not known to sign BAAs.

There's also a solution from Freshpaint that claims to scrub all personally identifiable information *before* it gets shared with Google and Meta. Its promises are interesting, but I'm not quite ready to endorse them.

Self-hosted alternatives to Google Analytics like Matomo and Piwik Pro are also attracting attention. They keep you in control of your data by never having it leave your possession. But they also come with pros and cons that you should investigate.

And, of course, some organizations will do nothing. That's highly concerning to me.

Surveying the landscape, Elizabeth Litten, Esq., chief privacy & HIPAA compliance officer at the highly respected Fox Rothschild law firm, has a similar take.

"OCR's new guidelines are helpful, but they also raise many interesting questions. They'll be addressed over time, but I'm recommending a conservative approach for most organizations until we know more," she told me. "I appreciate that these online tracking tools have business value, but the risk of an expensive and time-consuming enforcement action or civil lawsuit needs to be considered, too. Proceed with caution, I say."

Elizabeth Litten, Esq., chief privacy & HIPAA compliance officer at Fox Rothschild

I hope this article serves as a high-priority call to action for my fellow healthcare marketers.

In the best of times, HIPAA compliance is a complicated and high-stakes challenge. OCR's new privacy guidance is a clear sign that they'll be watching online tracking technologies with a heightened interest. Enforcement actions and civil lawsuits with serious consequences could come unexpectedly to the careless or unprepared.

I encourage you to move quickly, smartly, and with caution.

This article and the links provided are for informational use only and should not be construed as legal advice. Contact a qualified attorney to obtain advice specific to your situation.

James A. Gardner leads OHO Interactive's healthcare strategy practice, where he serves hospitals, health systems, and insurers across the country. He started his career with Procter & Gamble before earning his MBA at Northwestern University and serving clients as a consultant with McKinsey & Company. James is also adjunct faculty at Boston's Northeastern University.

Back to Table of Contents

WebMD Ignite Responds to Frequently Asked Questions About HIPAA and Tracking Technologies

By Jane Weber Brubaker

Have questions about how to manage tracking technologies in light of HHS/OCR guidance? So do your peers. Here are some answers from two technology leaders.

When HHS and OCR opened up a huge can of worms last December, they created some chaos in the universe of healthcare marketers who work for entities covered by HIPAA.

There's such a hunger for information and guidance. We're doing our part to feed the hungry, with articles and webinars that raise the red flags that healthcare marketers should pay attention to, to avoid a HIPAA breach — and a potential lawsuit — by sending protected health information (PHI) to a non-HIPAA compliant business associate.

As a frequent webinar moderator, I've noticed that when the Q&A starts, it's a signal to many people to drop off, now that the presentation is over. Not so with this topic. There's tremendous interest in diving deep.

In a recent webinar from WebMD Ignite, "Pixel Privacy Conundrum," the Q&A captured the major questions people have. The responses from the two presenters from WebMD Ignite, Andy Waldrop, vice president, digital experiences & production management at WebMD Ignite, and Josh Kinney, director of digital technology, were rich and detailed.

Before responding to any questions, Waldrop emphasized that the guidance is NOT legal advice. "It's up to each covered entity to decide their approach to compliance and appetite for risk," he says.

Here, we share a condensed version of the webinar Q&A.

Andy Waldrop, vice president, digital experiences & production management at WebMD Ignite

Q: Is Google Analytics (GA) HIPAA-complaint?

AW: The short answer is no. Google will not sign a BAA. It is not HIPAA-compliant. However, there are ways to limit the data it tracks.

Q: What is a balanced approach to GA4, which claims it doesn't track IP addresses? Are there other settings we can look at to be as anonymous as possible with user-generated data?

AW: With the correct governance applied to GA4, you can customize things further and mask what's being shared. The default cookie tracks a decent amount of information. While it is nice that they don't track IP addresses by default, there still can be room for device IDs or other personal information to be tracked, whether it's purposeful or inadvertent through search queries or other activity.

If you are going to use GA4, one approach is to treat it as a non-compliant cookie. Another is to make sure — for anyone who has access to your Google Analytics instance and any web property or mobile property where that information can actually fire — that what is firing is not tracking form fields where sensitive information is captured.

Q: When vetting a new analytics vendor, what are some good questions to ask?

AW: A great approach is to get different points of view. In our evaluations, we're bringing in a multi-faceted team — folks that spend their days on just SEO, or web development, or advertising and MarTech experts — so we have different perspectives.

A pivotal question is, will the vendor sign a BAA (Business Associate Agreement)? Are they mitigating the risk for you or will you still own the risk with maybe a way to make it compliant in your covered entity's view? Understand that there's a cost. Most vendors that are willing to sign a BAA are taking on some risk and there's a cost involved.

Some other things that are a little more technical to ask would be around the data model of the analytics platform. Is it full storage and retrieval of data? Or is the data aggregated?

If you have ambitions of building a data lake or other larger collection of data, does that analytics provider enable data extracts or ways to connect to data lakes like Snowflake or BigQuery?

And then for use case-specific tag management or event tracking, can I label the things I want to track? Or will that require technical resources? Some platforms are developer-friendly but almost impossible to use by a non-developer. Others favor the no-code approach. It's best to understand your team's use cases and skillset upfront to better evaluate potential solutions.

Q: As clean rooms are becoming more important for a cookie-less world, is this another area where a BAA needs to be considered?

AW: Yes, 100 percent. You should have an understanding of whether you have a BAA or not with that vendor. If not, what are you doing to ensure that patient data or sensitive data is not shared? And even if you have a BAA on a clean room or data lake, it does not protect every potential data source that's feeding into it.

Anywhere a covered entity is sharing data, whether it's through a cookie or a direct integration, it ultimately falls on the covered entity to make sure you are in compliance in your organization's view.

Q: How can I see what pixels are being used on my website right now?

JK: We usually look to some Chrome extensions. Ghostery is an old tried and true one. You can just turn it on, visit a website, and it'll pop up the different pixels that are placed on that site.

AW: Keep in mind these tools can also find things that are not third-party cookies, like versions of JavaScript or technology you use on your site.

Q: Do the OCR/HHS guidelines apply to all domains belonging to a covered entity or only the ones potentially used by patients? For example, would a recruitment job seeker site be included?

Josh Kinney, director of digital technology at WebMD Ignite

AW: Unfortunately, HHS did not answer questions like this, or questions about data sharing that is not cookie related. Ultimately, it's going to come back to your legal and compliance department to answer that.

Q: What would you guess is the ratio of healthcare entities taking a conservative approach vs. unrestricted?

AW: I think there's a lot of appetite for the middle of the road. But that takes some investment, when you need to capture some data and also mitigate risk.

Q: Can you give some examples of analytics solutions that will sign a BAA?

AW: I'll give you three that will sign. Heap Analytics will sign a BAA. Snowplow and Matomo Analytics allow you to self-host on your own infrastructure, so you can make them compliant. You would set up your own data storage in a compliant location on a cloud vendor or on-prem and then you use their visualization on top of it.

Keep in mind that these options are 100 percent analytics focused. They're not going to help you with Google ad tags, Meta tags, third-party tracking tags, or other ways you might want to capture or pass data.

Freshpaint has a BAA-supported healthcare privacy platform that enables users to govern data flow to third-party tools. The product gives healthcare companies control of data privacy by blocking PHI from being shared with tools that aren't HIPAA-compliant. Health

systems can continue using Google Analytics, Google Ads, and Facebook by replacing native web trackers and promoting HIPAA compliance.

JK: A lot of the focus has been around finding a Google Analytics replacement, but we found that the topic is a lot broader. Meta alone is a major marketing player that has a lot of litigation piling up against it. It really becomes a question of how to safeguard against any pixels that may or may not claim compliance.

Back to Table of Contents

5 Strategies for Measuring ROI and Growth: It's Not Only About Tracking Pixels

By Shawn Gross

Health system marketing is more than gathering marketing pixel data — it's about creating measurable business growth that offers real value and builds long-term loyalty.

Amid the turbulence of healthcare privacy reforms, marketers are caught up in a tug of war between adherence and effectiveness.

While debates about tracking pixels, OCR's guidance, and evolving state regulations dominate the conversation, it's essential that we keep our eyes on the primary objective: reporting marketing's tangible ROI and effectiveness in driving business growth to C-suite executives.

Beyond Pixels: Broadening the Horizon

Today's privacy discourse, saturated with the intricacies of tracking pixels and data security, misses the forest for the trees. It's not just about gathering personal user data but about creating meaningful experiences that connect with people during life's biggest moments.

The main goal of health system marketing should be about establishing impactful relationships between your brand and patients, caregivers, jobseekers, donors, researchers, and more, while measuring the effectiveness and modifying tactics based on real-world feedback and outcomes.

Here are five strategies for health system and hospital marketers to develop a comprehensive plan that establishes and reports on marketing's impact without an overreliance on tracking pixels. There's just one catch — it's going to require building stronger collaborations outside of marketing to thrive.

Still have pixel questions? We've also included a sidebar with suggested actions for managing privacy issues related to tracking pixels.

1. Downstream Patient Revenue: The Heartbeat of Healthcare ROI

- **A vital role:** Healthcare exists to serve patients. If your marketing funnels more patients toward your services, it's succeeding in its primary task. More admissions translate to increased revenue, which is directly attributable to SEO, marketing campaigns, your website, and mobile app.

- **Detailed metrics:** It's critical to establish an attribution model that ties organic and marketing campaign-driven traffic to tangible results: patient admissions, surgeries, or diagnostics.

Focus on the entire patient journey, from the initial search on a health condition to the final booking of an appointment. Harness the capabilities of CRM systems that merge seamlessly with your hospital's EMR to pinpoint the connection between marketing actions and patient interactions.

Still trying to work with other departments to automate attribution? Don't let waiting for an enterprise CRM rollout stop you. Take an initial step by scheduling monthly meetings with participating clinical operations teams. I did this at Tufts Medical Center and, surprisingly, this manual tracking process worked. Paid search ads, SEO, tracking appointments via phone numbers collected from a web form, and a giant paper shredder are key to success.

- **Channels impacted:** Digital reigns supreme here. Think search engine marketing, SEO, retargeting campaigns, online appointments, and unique content experiences that prospective patients would share their contact information to use.

2. Customer Satisfaction: Beyond Numbers, Emotions Matter

- **Recognize its significance:** Satisfaction cements loyalty. Every delighted patient or family member becomes an advocate for your services, often leading to referrals and word-of-mouth promotions.
- **Delve deep:** Use post-treatment surveys and online reviews as metrics. Incorporate feedback modules within your digital platforms, relating satisfaction scores with specific marketing touchpoints. This will enable targeted improvements.
- **Traditional channels**: Radio and print are unaffected by rapidly changing digital privacy reforms.

3. The Generosity Index: Tying Marketing to Increased Donations

- **Significance:** In the world of healthcare communications, philanthropy is pivotal. Marketing can significantly bolster hospital finances by creating unique digital engagement experiences that generate personalized calls to donate, effectively intertwining patient and innovation success stories, and transparently reporting how individual gifts impact care.
- **Measurement:** Examine donation patterns before and after significant campaigns. Use special URLs or QR codes exclusive to campaigns to gauge direct responses. Launch new programs that help contributors make giving an integral part of everyday spending (e.g., rounding-up initiatives), where donors are motivated to support your brand without ever having to be asked.

- **Channels:** Leverage the personal touch of email marketing, the relatability of social media patient stories, and evocative, transactional-driven mobile content marketing.

The Changing Privacy Landscape details the current state of affairs with Google and Meta tracking pixels, and offers best practices that marketing teams can immediately implement. Here are some suggested actions:

- In some instances, it's still okay for healthcare organizations to stick with Google Analytics. Check with your privacy team. And if not, here are three other options for partners/vendors: PiWik Pro, Mamoto, Adobe.
- Audit your analytics property for possible PHI data.
- Audit your website for possible PHI leaks. This should not be a one-and-done practice.
- Audit your analytics for user visits from the European Economic Area countries to determine GDPR requirements compliance.
- Review your website privacy policy to ensure that it aligns with current marketing activities; update it to include required GDPR language, especially around your legal basis for capture of user information.
- Update any static cookie notification banner to a managed consent solution.
- Update website forms to require users to acknowledge that they have read the website privacy policy, and state that submission does not constitute establishment of a patient/provider relationship (for HIPAA).
- Review CCPA, CPRA, CPA, CTDPA, UCPA, and CDPA territorial scope and application threshold to determine if California, Connecticut, Utah, Virginia, and Colorado state privacy laws apply.
- Conduct data discovery with your IT department to map where all user data is currently retained as well as who has access to this data, including employees and external partners.
- Determine what data is being captured by the marketing pixels you have implemented on your site. Be sure to disclose this in your privacy policy.

Source: Primacy

4. Building the Team: Linking Marketing to Recruitment

- **Why it matters:** A thriving hospital depends on its staff. By showcasing institutional milestones and nurturing workplace-of-choice culture through campaigns, you attract talent.
- **Metrics modus operandi:** Scrutinize the spike in applications and hires after specific recruitment drives. LinkedIn, with its analytics, is a gold mine for tracking the efficacy of recruitment content.
- **Recruitment beacons:** Strengthen you presence on online job portals and through LinkedIn promotions, career fairs, and the employment sections of official hospital websites. Launch new programs like Talent Communities, where candidates express interest *before* new jobs are posted.

5. Research Funding: Marrying Innovations with Investments

- **Decoding its importance:** Advancement in healthcare is tethered to research. By highlighting institutional research achievements, marketers can work with research institutes and labs to attract potential funding, thereby catalyzing further innovations.
- **Tracking techniques:** Engagement metrics on research publications, juxtaposed with funding patterns, can reveal correlations. Monitor interest levels from potential investors or partners after campaigns focused on research breakthroughs.
- **Key channels:** Extend your influence through PR, academic journals, proprietary hospital research publications, and research-centric seminars or webinars.

The approaches discussed in this article ensure that marketing is focused on initiatives beyond tracking patient appointments. New measurement ideas require cross-department collaboration in an ever-changing healthcare landscape where growth measurement and marketing ROI aren't always clear.

By constantly evaluating the impact of new tactics, health system marketers can better align their strategies with the evolving needs and preferences of their target audiences and internal stakeholders, ultimately driving end-user satisfaction and organizational business growth.

Navigating the maze of healthcare marketing in these transformative times is undoubtedly challenging. But by centering our efforts on healthcare's key pillars of service, care, and innovation, we not only adapt to market shifts but also position ourselves as change agents best capable of measuring marketing's transformative business impact.

Strategies to Champion:

1. Transition from a siloed patient acquisition-specific mindset to a comprehensive multi-audience growth model. This comprehensive view is crucial for ROI clarity.
2. Enterprise CRM still in the works? Pilot a few service lines and manually track new patient appointments, donations, new hires, and more.
3. Get outside the confines of what marketing generally takes responsibility for by continuously engaging and educating stakeholders on the evolving topic of healthcare ROI. Migrate from impressions and click rates to robust indicators like patient admissions, customer satisfaction, donations, recruitment, and research funding.
4. Regarding tracking pixels, privacy, and digital experience personalization, cultivate a culture of periodic reviews across all your teams. Privacy policies and data collection techniques need to continuously adapt, reflecting legislative mandates, overarching organizational objectives, and the needs of your end users.

Shawn Gross is health practice lead for Primacy, a data-inspired, full-service digital agency that creates meaningful experiences that connect with people during life's biggest moments. Follow Shawn on LinkedIn.

Back to Table of Contents

Solving the HIPAA Conundrum

By Jane Weber Brubaker

Can healthcare marketers leverage tracking technologies the way they used to without risking noncompliance?

When HHS stepped on the gas last December — issuing ominous warnings about HIPAA, tracking pixels, and PHI — healthcare marketers and legal and compliance teams put the brakes on fast. But some organizations had already been called out for HIPAA breaches related to third-party tracking tools like Meta Pixel and Google Analytics.

Dozens of high-profile lawsuits put noncompliant health systems in the crosshairs, but the fact is that most U.S. health systems are at risk. Authors of a study published by *HealthAffairs* in April reported, "We found that third-party tracking is present on 98.6 percent of hospital websites, including transfers to large technology companies, social media companies, advertising firms, and data brokers."

Just when marketers were finally able to improve website experience, monitor campaigns using real-time analytics, and prove ROI, the door to the enabling technologies and high-performing ad platforms slammed shut in their faces.

Enter new technology solutions designed to solve the tracking pixel problems. We met up with one of them, Freshpaint, at a sunrise session at SHSMD Connections in Chicago. In spite of the early hour (7 a.m.), the room was packed, with standing room only. Marketers clearly are interested in finding a way to get back to business AND comply with HIPAA's guidance on PHI.

Ray Mina, head of marketing at Freshpaint

Ray Mina is head of marketing at Freshpaint. "There's a whole bunch of technology that you utilize on your website, whether it's for acquisition, for analytics and measurement, or to improve the customer experience," he says, "and those tools are powered by trackers — snippets of code that sit on your website — and those snippets of code do some things that have the regulators concerned."

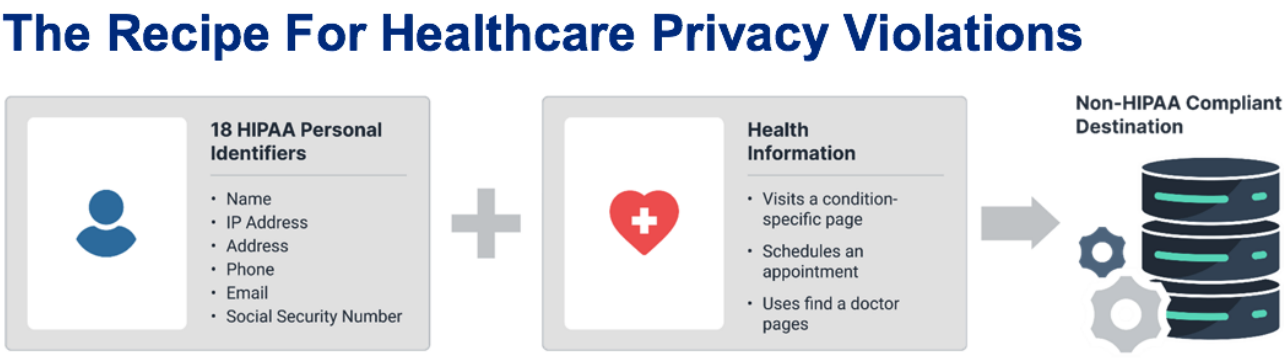
Here, we recap the issues and potential pitfalls, as well as workarounds that Mina suggests can help marketers take charge again and restart measurable, trackable, and effective marketing, in compliance with HIPAA.

The HIPAA Privacy Rule specifies 18 identifiers of people, including "relatives, employers, or household members" of those people, that covered entities must de-identify when sharing PHI. The list is granular, covering not just obvious clues to someone's identity like their name or email address, but also anonymous identifiers like URLs and IP addresses.

Mina explains three necessary ingredients for PHI: "In order for it to be protected health information, the first thing it has to have is an identifier. If you have an IP address, literally every tracking technology in the universe — that's how the internet works — collects an IP address."

The second component is health information such as a site visitor using the Find a Doctor page or searching for information on treatments.

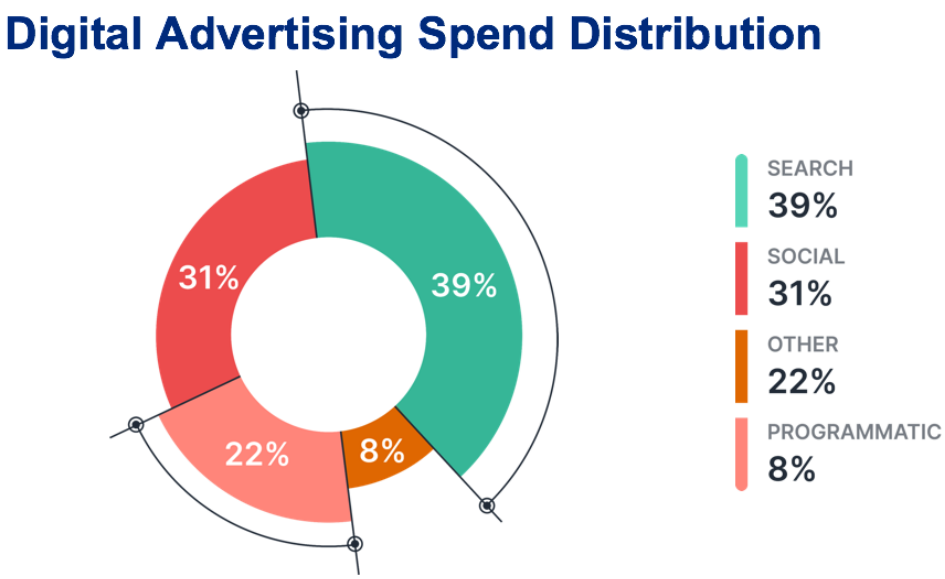
A HIPAA violation occurs when an organization shares these two pieces — an identifier plus health information — with a third-party that hasn't signed a Business Associate Agreement (BAA) with the organization. HHS states: "The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information."



A HIPAA breach occurs when an identifier and health information are shared with a non-HIPAA-compliant entity.

Risks of Noncompliance

One problem for healthcare marketers is that a large chunk of digital advertising consists of paid ads on Google and Facebook. By loading a snippet of the ad platforms' JavaScript code onto their organizations' web pages, marketers can track and measure the effectiveness of the ads.



This all blew up when The Markup tested 100 U.S. hospital websites in June 2022 and found Facebook's Meta Pixel on 33 of them. Whenever visitors clicked a "schedule an appointment" button, for example, Facebook received that information along with the visitor's IP address. This resulted in PHI being sent to Facebook, which then used it to refine its ad targeting capabilities. Since Facebook is not HIPAA-compliant, and does not sign BAAs, any hospital allowing that information to flow to Facebook is in breach of HIPAA and at risk of being sued.

Meta now faces a class action suit that it has tried unsuccessfully to have dismissed. The HIPAA Journal states: "The lawsuit alleges that Meta knew, or should have known, that the Pixel tool was being used improperly on the websites of hospitals. The lawsuit alleges at least 664 hospital systems and medical providers were sending medical information to Facebook through the Meta Pixel tool."

But Facebook's Meta Pixel is just one tracking tool. Many others such as Google Analytics are widely used. Hospital and health system websites no longer can claim ignorance. They will be held responsible for HIPAA breaches related to any tracking pixels on their websites. The Office for Civil Rights stated in its December 2022 Bulletin: "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

Enable Tracking Without Triggering a Breach

Freshpaint describes itself as "the industry's first healthcare-focused offering for HIPAA compliance, with a data governance toolset to control sensitive data like Protected Health Information (PHI) across a stack of analytics and marketing tools."

"We've been working with probably hundreds of healthcare providers since December's HHS guidance came down," Mina says. "We sign a BAA with all of our healthcare customers."

A high-level description of the solution is that it is a protective layer between client-side websites and the technology platforms they send data to — advertising platforms like Google and Facebook, analytics tools, and video platforms like YouTube and Vimeo — where there is no BAA in place.

Mina suggests that customers begin by auditing their websites. "You need to get a general inventory of what trackers you are running. There are some free tools out there where you could actually scan your site, but I would recommend a more thorough search by recruiting someone from the IT team."

Customers should then determine if that tracker shares PHI. "This is where you'll need to partner with your legal compliance team to have those conversations," Mina says.

The next step is determining where there are PHI risks. Mina explains, "You need to verify that it's okay for that tracker to collect and share PHI. Do you have a BAA with that tool where this data is ending up? Inevitably, you are going to end up with a subset of tools that you either don't have a BAA or don't need a BAA."

Mina thinks it's unlikely that Facebook and Google will ever sign a BAA with healthcare organizations. But healthcare marketers can still use these platforms without risking noncompliance with HIPAA by removing native trackers and replacing them with trackers from a solution that has a BAA behind it, such as Freshpaint.

"You replace all of those tracking pixels with one," says Mina, "and then we actually can safely collect data from your site. All non-HIPAA compliant tracking technologies will never have access to sensitive information on a healthcare website."

Marketing and legal and compliance teams can then use a visual interface to opt in or opt out of sending certain types of information. "For example, you are clearly never going to opt-in to send an IP address or device ID to an analytics tool that has information about the context of your healthcare website," Mina says. The benefit is that they don't have to rely on engineering resources for custom coding.

Similar logic applies to Google Tag Manager. Tags are converted to Freshpaint tags and governed through the same visual interface.

To retain the ability to understand a site visitor's journey history, enabled by Google Analytics, Freshpaint creates an anonymous ID. "Google [Analytics] has no way of knowing who the visitor is, but they know that it is the same visitor, and they can actually stitch together that entire journey."

Workarounds for Ads

Regarding ads, Mina says, "This will probably be the stickiest part of any conversation you have with legal and compliance because ads do require identifiers."

He explains that programmatic advertising depends on a seed audience. "So, the first 30 people that scheduled an appointment, they need to know who those people were," he says. "If you remove the tracker and you remove that feedback, the whole thing breaks down."

To make it work again, Mina says two pieces of data are needed:

1. That a conversion happened — make it coded, but don't name it something that would introduce health information, like "scheduled appointment."
2. An ad click ID with information about the ad and the campaign.

With this information, the ad platform can use machine learning to find more people who match.

One unnamed Freshpaint customer — a regional healthcare organization with 4,000 physicians — was able to collect more data because it was able to safely place tracking pixels on more web pages. "They feel like there's actually a new opportunity to measure their conversions further downstream and get closer to what their return on investment is," says Mina.

The risks of HIPAA noncompliance are too great to ignore. Mina cautions, "If you have these pixels and trackers on your website, think of it as a signpost for regulators and lawyers to dig deeper."

Back to Table of Contents

Traffic Risks: Next Steps for Tracking Pixels and HIPAA Compliance

By Elaine Christie

Digital marketing got a lot riskier when HHS rolled out its "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" bulletin last December. What steps should you take to manage the risks?

Change often feels like the only constant in the world of healthcare marketing. And oh, what a year of change! At the end of 2022, the Department of Health and Human Services (HHS) released new guidance about HIPAA, online tracking, and consumer privacy. Less than eight months later, HHS and the Federal Trade Commission (FTC) published a joint letter that included FTC actions against sites like Easy Healthcare, BetterHelp, GoodRx, and Flo Health. The letter indicates that HHS and the FTC are in lockstep in their views on how the guidance should apply to protect PHI.

Some might say that HHS and FTC have valid reasons for pushing healthcare organizations to take actions to protect the privacy and security of individuals' health information. Earlier this year, we reported on the websites at 100 prominent hospitals that had user tracking technology from Meta (the parent company of Facebook). The tracking technologies allegedly captured data about pages visited, searches conducted, and appointment scheduling. Meta's advertising algorithms were synced to consumers' searches for specific health conditions or highly private concerns.

How Hospitals Are Responding to New Ad-Tracking Rules

Ben Dillon has spent the better part of the past eight months interviewing the compliance and legal teams at dozens of healthcare organizations. Dillon, co-owner and chief executive officer of Geonetric and a member of the *eHST* Editorial Advisory Board, set out to find out what these organizations are doing to ensure compliance. He identified a wide range of interpretations of the new ad-tracking rules.

Dillon untangled some of the mysteries that are puzzling today's healthcare marketers in a recent eHST webinar, "HIPAA-Pocalypse Now: Understanding the New HHS Guidance, the Implications for Healthcare Digital Marketers, and How to Respond."

Ben Dillon, CEO and co-founder, Geonetric

Read on to learn how to assess your current situation, protect your patients' privacy, and help your organization steer clear of HIPAA violations.

What Are the Risks of Tracking?

First, it's important to understand the evolving rules about sending protected health information (PHI) to a non-HIPAA compliant third party. PHI is anything that can be used to identify a patient, such as names, addresses, Social Security numbers, and health records. But HHS lists 18 separate identifiers, including device attributes or serial numbers; digital identifiers, such as website URLs; and IP addresses. While IP addresses have often not been considered unique identifiers by healthcare organizations, the new guidance makes clear that this should be the case in the future. Furthermore, the guidance says that having an IP address or other identifier of a person along with the URL of a page on your website runs the risk of being PHI.

In essence, HHS and FTC are saying that ignorance isn't bliss and you're still liable —

- whether or not you are a regulated entity under HIPAA.
- whether or not you use the data obtained through tracking technologies for marketing purposes.
- whether or not you're aware that you're leaking sensitive data.
- even if you hired someone else to design your website or build your app.
- even if you didn't know about tracking tools.

Let's take something as innocuous as a form submission. Imagine that your website uses tracking pixels alongside contact forms, appointment requests, or patient feedback forms. There is a risk that patients might input PHI into those forms — and the tracking pixel might capture this data if not configured properly.

Dillon touched on this scenario during the webinar. For example, if these tools are HIPAA-compliant, and you don't have random third parties who may have access to information, people voluntarily submitting information is probably fine.

"When you're pushing stuff to analytics and things like that, that's where you start to get into trouble," says Dillon "So, if someone's volunteering information to you, that doesn't mean that they're volunteering information to Google or Facebook or your retargeting platform."

Watch the full webinar here: HIPAA-Pocalypse Now: Understanding the New HHS Guidance, the Implications for Healthcare Digital Marketers, and How to Respond

Dillon noted that some organizations have even debated the idea of having people "sign off" on HIPAA — in essence, giving their explicit permission for that data to be sent to third parties.

"But HIPAA requires a separate authorization for each use of a consumer's data. That means you'd need one for Facebook, one for Google, one for this, and one for that — which is awkward. I think most organizations have ultimately decided that it's probably not manageable or would be too disruptive to the consumer experience," he says.

What about using QR codes to direct consumers to your website from various forms of offline marketing? Although QR codes can provide insightful reporting and marketing metrics, proceed with caution.

"The core technology of QR codes is not fundamentally flawed. I think you just have to be careful about third-party involvement. A lot of these tools have gotten more sophisticated over time. When someone hits that QR code, it's not going directly to your URL, it's going to a third-party platform. The trouble is, the third-party agency is now collecting all kinds of good information about the patient's physical location, their device, the time of day, and so on," says Dillon.

"When it's bouncing off of a third party, you need to be careful. If you can, get a QR code that actually just gives the link to your site, and is not going through some kind of third party," he adds.

What about linking to YouTube videos? Dillon urges caution about any third-party service that might be receiving data from your digital properties including embedded YouTube videos.

"Once you start digging into your sites, you find the sheer number of different places where you're touching outside stuff. One example is embedded YouTube videos, which can be a potential risk. In this scenario, YouTube offers a privacy-enhanced mode, which significantly reduces the amount of data going back and forth before your site visitor makes a choice to view the video," he says.

Should you be concerned if your website offers an online appointment scheduler? The answer is — it depends. Dillon recommends first looking at the platform and where it's hosted.

"Go through and do a holistic assessment: What data is getting pushed out to third parties where you don't have a BAA in place? Certainly, if it's dealing with scheduling appointments and you're sharing IP addresses and URLs with such third parties, that could be problematic. You need to look carefully at that and make some hard decisions," he says.

Anything Touching Live Traffic Represents a Risk

Engaging in a risk assessment process will help you develop a process for achieving and maintaining compliance."Audit everything touching live web traffic for patients and/or consumers. What data is going where? Look at each of those items to determine risk," Dillon recommends.

As one example, Dillon looked at the FTC's recent action against GoodRX. He says it's the first time the rule is being employed in an enforcement action and the first time a proposed FTC consent order is being used to prohibit a company's use of consumer health data for advertising purposes.

According to the FTC claims, GoodRX allegedly:

- Shared PHI with Facebook, Google, Criteo, and others.
- Promised users that it would never share PHI with advertisers but violated this promise.
- Failed to limit third-party use of PHI.
- Misrepresented its HIPAA compliance.
- Failed to implement policies to protect PHI.

"The nature of the internet is that so many things are leveraging persistent services that are out there in the world. You need to look at each and every one of those," Dillon emphasizes.

Watch the full webinar here: HIPAA-Pocalypse Now: Understanding the New HHS Guidance, the Implications for Healthcare Digital Marketers, and How to Respond

4 Compliance Tips

1. Stay updated on HIPAA regulations.

- Study how they apply to your specific role as a healthcare marketer.
- Ensure you understand the Privacy Rule, Security Rule, and any other relevant provisions.

2. Select HIPAA-compliant tracking tools.

- When choosing online tracking technologies, seek out tools that protect against the unauthorized disclosure of PHI.
- Work closely with your IT or security team to make sure you're using appropriate tools.

3. Audit to understand all of your points of risk.

- Execute BAAs with the platforms that will do that
- Assess risk of those who won't and implement a Mitigation plan
- Remove
- Replace
- Anonymize

4. Implement a long-term vendor/partner management program.

Final Thoughts

The big takeaway from the webinar? Just because someone shares their information with you doesn't imply permission for you to share it with anyone else.

As you continue to learn about the evolving landscape of healthcare marketing and online tracking technologies, remember to stay in close touch with your legal and compliance teams.

Finally, remember to look beyond pixels once in a while. Your primary goal is to create authentic, vibrant relationships with patients. As discussed earlier this year, an overemphasis on tracking pixels and data security might be missing the forest for the trees. As a health system marketer, it's important to find the balance between authentic relationship-building and tracking analytics. Only then will you be empowered to create long-term loyalty that embodies HIPAA compliance at its core.

Elaine Christie is a trained journalist, technology advocate, and frequent writer about digital transformation, internet marketing, and cybersecurity.

Back to Table of Contents ▲

Exploring Privacy Enhancing Technologies as a Potential Solution to Privacy in AdTech

By Jane Weber Brubaker

Advertisers are highly motivated to find ways to take full advantage of digital marketing — without triggering a privacy breach. The AdTech ecosystem is just as motivated to find solutions, with billions of dollars in ad revenue at stake.

Healthcare marketers have been scrambling to find ways to reclaim the data analytics they've grown accustomed to while also staying in compliance with HIPAA and its latest dictates, published in a bulletin from HHS last December. On the other side of the fence, the AdTech world has been working just as feverishly to retain its attractiveness to digital marketers and protect consumer privacy.

Privacy Enhancing Technologies, or PETs, is an umbrella term covering a variety of technologies that can be used alone or in conjunction with others to protect privacy. According to Clearcode, "PETs are designed to help companies protect user privacy while still enabling them to collect and use data for programmatic advertising."

Some examples of PETs include differential privacy, on-device learning, K-anonymity, and secure multi-party computation.

The U.S. Census used differential privacy in the 2020 census with the goal of providing statistics in aggregate while preventing the possibility of reverse engineering the data to discover personal information. The technique involved introducing "noise" into the system, or computer-generated inaccuracies designed to protect confidentiality. A 2022 New York Times article, *The 2020 Census Suggests That People Live Underwater. There's a Reason,* states, "Differential privacy algorithms can be tuned to meet precise confidentiality needs," suggesting that the level of noise can be turned up or down to achieve the target.

Anthony Katsur, CEO, The IAB Tech Lab

The IAB Tech Lab, an independently-governed branch of IAB (Internet Advertising Bureau), created the PETs Working Group in February 2022 to explore potential use cases for PETs in digital advertising. To learn more about PETs and the current state of evolution in AdTech, we spoke with Anthony Katsur, CEO of IAB Tech Lab. In the interview that

follows, Katsur gives an overview of PETs and discusses how these technologies can protect consumer privacy. [Edited for clarity and brevity.]

eHST: Why did the IAB Tech Lab decide to pursue a privacy-enhancing technology initiative?

AK: There are several reasons. The internet's growth has been largely funded or subsidized by advertising. The web's growth is largely ad dollar supported, more so than any subscription that you use to access content. It's more than 50 percent ad supported.

And the reason is because the internet has represented a higher fidelity form of addressability than traditional forms of media — television, print, out of home. Probably the closest thing in terms of addressability is direct mail. Direct mail continues to thrive in this digital world because it's highly addressable. You can message a set of cohorts, you can modify your messaging based on the cohort, you can offer different products and services based on the cohorts. It's much more precise.

eHST: Where does privacy come into the picture?

AK: With the advent of recent privacy regulation, everyone thinks that privacy regulations just started. They haven't. HIPAA was one of the earliest privacy regulations around, so these privacy regulations aren't anything new. However, in order for the industry to come into compliance with a lot of these regulations, you've got to look at the spirit of the regulations beyond just the law. And what's the concern? I think governments around the world have a concern around consumer privacy and data security. We've conflated those two things.

In this video Katsur explains how PETs, by their nature, can protect consumer privacy

eHST: Is IAB Tech Lab's position different?

AK: Our belief is that consumers either explicitly or implicitly realize the trade-off of sharing information about themselves with the internet. They get access to either free or cheaper services because of that advertising subsidy. However, consumers become much more concerned about privacy when there's a data security issue. The minute there's a data breach, that's when consumers get concerned about their privacy or their data.

The reason we introduce privacy enhancing technologies is we see that as a means by which we can protect the consumer's privacy right out of the gate. Privacy enhancing technologies effectively obfuscate and destroy any of the source sensitive personal information that may have gone into building a consumer cohort model. So immediately, you've got consumer privacy protections.

Given the nature of how privacy enhancing technologies work, it becomes near impossible to trace anything back to an individual email address, or any form of SPI [sensitive personal information] when you apply PETs to the source data.

The second half of this is that PETs are also inherently data secure. It's very hard to reverse engineer it. So, if you are applying some form of PETs to your data sources, whether it be multi-party compute, differential privacy, some form of K-anonymity, and that data source — after it has been through a PETs process — is breached, it's still highly data secure. There's inherent consumer privacy built into it if you're applying PETs.

eHST: There are a number of different forms of PETs. Is the PETs Working Group focusing on all of them?

AK: We are focused on secure multi-party compute and differential privacy for advertising use cases. Once that has all been applied, it's inherently a data-secure asset that still supports some form of addressable advertising across the internet, without there being consumer privacy or data security issues. So that that was the whole premise of why we started to look at PETs

eHST: Are there examples of how these techniques are being used?

AK: We've seen privacy enhancing technologies used to great effect. The U.S. Census used differential privacy for its census data in order to protect consumer privacy. At the height of COVID, Apple and Google used concepts like on-device compute and differential privacy in conjunction with each other to create the exposure tracker, without tying it back to any sort of personal information.

I'm going to radically simplify how this worked. With on-device compute, the data never leaves the device That's the first level of data security. Now, if one were to apply differential privacy to the on-device data, that would add sufficient noise to the data that it would blind anyone from reverse engineering that to a specific device, but if you were to compare and

contrast those on-device data sets, you would get strong enough signal that a device was exposed to COVID.

So, PETs aren't new to certain industries. I would say they're relatively new to the digital advertising ecosystem.

eHST: What is the intersection of PETs and the issues around tracking technologies and PHI?

AK: I think where they intersect is that the concept of PETs very often deals in the world of aggregate data. Let's just say you're creating an aggregate data set. When you're using differential privacy to introduce noise into that aggregate, that becomes very hard to reverse engineer to an individual.

eHST: I've asked healthcare marketers if they know anything about PETs and the answer has been no. Why do you think that is?

AK: Because it is early. If you look at privacy enhancing technologies as a practice, across all industries, it's still relatively early, maybe a decade where at least the concepts have been there. K-anonymity is not a new concept, differential privacy is not that new.

I'd like to see greater involvement from the healthcare industry in what we're doing. I think they would bring even more knowledge and perspective because of the level of scrutiny they're under. Healthcare data protection laws have been in place much longer than general data protection laws. I think they would bring an advanced understanding of how they define and see compliance with privacy law.

eHST: If you were going to lead a webinar for healthcare marketers who are trying to figure this out, what would you include?

AK: I think there are three components. One is opening with a fundamental understanding of some core PETs concepts — a layman's explanation of the top three or four PETs concepts and how they're used to protect information

And number two I would lay out the practical operations in terms of how those can be leveraged today in digital advertising, including healthcare marketing, everything from audience activation and management using PETs, but also, how do you then do attribution and understand campaign performance in a PETs-powered advertising campaign?

Phase three would be understanding the future of PETS — practical examples of how you would activate PETs in healthcare marketing. Here's how you can actually put it to use, these are some best practices around using it. For example, you should double blind your data at all times. You should have already applied PETs to your core datasets — that creates that double blinding.

eHST: Who would be the appropriate people in healthcare organizations to be involved in a discussion of PETs as related to advertising?

AK: I think it's definitely the CMO and the CIO. I would involve constituents from their data security teams. And again, I think it's just starting with a one-on-one level education on privacy enhancing technologies. Here's how they work. Here's what they do. Here's how they work in conjunction with each other. I think it's starting with how PETs can help bring you into compliance with HIPAA.

eHST: Would you be interested in having healthcare marketers join IAB Tech Lab's PETs Working Group?

AK: If there are healthcare professionals who want to understand this more deeply, by all means connect with me. We can see if they want to join the Tech Lab as general members. Our membership fees do not break the bank. We'd love to have them join as members of the Tech Lab, and we can spend some time educating them on PETs.

If you are interested in learning more about the Privacy Enhancing Technologies Working Group, or joining, email: membership@iabtechlab.com.

Free Upgrade to Group Membership

Add Your Entire Team to Your *eHealthcare Strategy & Trends* Membership For No Extra Cost

With a group membership, your entire team — up to 9 additional members — get their own member accounts. Each member gets his or her own log in, providing access to every aspect of ehealthcarestrategy.com.

It's an amazing value. Seriously, where else can you train your entire team for a year for under $300?

Make your job easier. Train junior staffers in best practices. Keep your senior team up to date. Give them access to the latest developments and cutting edge strategies from the best minds in marketing, strategy and communications for hospitals, health systems and other healthcare organizations.

Already a member?
Log in now and manage your group members.

Not a member yet?
Sign up now with our low individual rates and then add your team members for no additional cost.

I urge you to take advantage of our complimentary group upgrade today. It's a great way to set your team up for a full year of learning and exciting successes — and this offer may not last long.

Sincerely,

Matt Humphrey
President
Plain-English Health Care
Publisher of *eHealthcare Strategy & Trends*